An Implementation Paper on VigilAI: Smart Border Surveillance System

Mr. Rushikesh Pimple[1], Ms. Bhagyashali. B. Kokode[2], Ms. Sanjoli Sharma[3], Mr. Reetik Bhandari[4,]
Mr. Satyam Shrivastav[5,] Ms. Alisha Tighare[6]
[1,2,3,4.5.6] *Computer Science and Engineering, PCE, Nagpur*

***Abstract*—This paper presents VigilAI, a real-time intelligent surveillance system designed to improve border security using computer vision techniques. Traditional surveillance systems depend on manual monitoring, which can lead to human error and slow response times. VigilAI solves these issues by integrating motion detection, face recognition, object detection, and multi-level threat classification into a single system. The proposed system uses background subtraction for efficient motion detection and face recognition to tell apart authorized and unauthorized individuals. It also employs a lightweight YOLO-based model for object detection to identify vehicles and animals. A high-priority threat detection module helps identify weapons, allowing for immediate alerts. The system includes a multi-level alert system that features buzzer alarms, snapshot capture, and real-time email notifications with location and timestamp information. Designed for low-cost deployment, VigilAI runs efficiently on standard hardware without needing high-end computational resources. Experimental results show that the system successfully detects intrusions and responds in real time, making it suitable for use in resource-limited and remote border areas.**

***Index Terms*—Border Security, Artificial Intelligence, Computer Vision, Face Recognition, Motion Detection, Real-Time Surveillance.**

I. INTRODUCTION

The border security situation has become a pressing concern in recent times owing to the rising threats in the form of illegal infiltration, smuggling, and other illicit activities. Conventional surveillance technologies rely on the continuous observation of video feeds by a human observer, which might lead to inattention and the overlooking of crucial events.

The emergence of computer vision and AI technologies has paved the way for the development of automated surveillance technologies. However, the majority of the surveillance technologies in use today rely on deep learning technologies, which require high-end infrastructure and thus cannot be implemented in remote areas.

This paper proposes a novel and efficient surveillance technology named VigilAI. The proposed system comprises a range of features such as motion detection, face recognition, object detection, and alert mechanisms, thereby providing a comprehensive surveillance system.

The main aim and objective of the proposed system, VigilAI, is to identify suspicious activities and take instant action by sending out alerts.

II. LITERATURE REVIEW

Surveillance systems are playing a significant role in maintaining the security and safety of the public, borders, and infrastructure. However, with the increase in the number of security threats such as illegal intrusions, smuggling, and other illicit activities, the traditional surveillance system based on continuous human observation has proven to be inefficient and inaccurate. Human observation sometimes leads to human error and delayed responses. Hence, to overcome the limitations and disadvantages associated with the traditional surveillance system, researchers have been keen on introducing intelligent surveillance systems based on computer vision and other intelligent technologies.

2.1 Anomaly Detection in Surveillance Systems:

Anomaly detection is the process of detecting patterns or behaviors that are different from the normal or expected behavior. For instance, in video surveillance, the anomalies detected by the system would be

suspicious movement, intrusion, or other abnormal behaviors in restricted areas. However, in the past, the system was based on human observation, which was a time-consuming and inaccurate process. Hence, the automated system was introduced to increase the accuracy and efficiency of the surveillance system. The existing research on anomaly detection has been categorized into reconstructive and predictive approaches.

2.2 Reconstructive-Based Approaches:

In the reconstructive-based approach, it is assumed that the trained model with normal data can reconstruct normal events with high precision. However, abnormal events will have high reconstruction error. The autoencoder is the most commonly used approach in reconstructive-based methods. The autoencoder is trained in such a way that it learns the compressed representation of the normal frames. The reconstruction error is used as the key factor in determining the abnormal frames.

Another approach used in anomaly detection is the Generative Adversarial Networks (GANs). The GANs consist of two components: one is the generator, which tries to reconstruct the normal frames; the second one is the discriminator, which identifies the normal or abnormal frames. Although the reconstructive-based methods have shown significant performance in anomaly detection, the need for large data and high computational power is the key limitation in using these methods. The time required in the training process is quite high. The deployment of these models in real-time systems is quite challenging.

2.3 Predictive-Based Approaches:

Predictive methods are based on the prediction of temporal patterns in the video stream. These methods predict the next frames based on previously seen frames. Any difference between the predicted frames and the actual frames is treated as an anomaly.

Methods like Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Convolutional LSTM (ConvLSTM) are used for predictive methods. These methods are effective in dealing with motion patterns. However, predictive methods have their own set of problems, like high memory requirements, slow processing speeds, complex training mechanisms, etc. These problems make predictive methods less suitable for surveillance systems.

2.4 Deep Learning-Based Surveillance Systems:

Deep learning techniques have improved the efficiency of surveillance systems. Convolutional Neural Networks (CNNs) have been used in the fields of object detection, face recognition, and activity classification. YOLO (You Only Look Once), SSD (Single Shot Detector), and Faster R-CNN have been used in the real-time detection of objects. Many researchers have proposed AI-based border surveillance systems that include the integration of video capturing, object detection, face recognition, and alert mechanisms. The proposed system shows high accuracy with rapid response times. Most of the deep learning-based systems require powerful hardware with high energy consumption. They require complex setup procedures. Deep learning-based systems can be considered black boxes. They cannot be understood in detail. Privacy is another issue with these systems. They involve the constant recognition of faces.

2.5 Traditional Computer Vision Techniques:

Before the era of deep learning, traditional computer vision techniques have been employed in various surveillance systems. These include techniques such as background subtraction, differencing, optical flow, and Haar cascade classifier. Background subtraction techniques, including Gaussian Mixture Models (GMM), are employed to detect moving objects based on the static background. Haar cascade classifier and Histogram of Oriented Gradients (HOG) with Support Vector Machines (SVM) are employed to detect faces. Although these techniques do not guarantee the same performance as deep learning techniques, they are computationally efficient and faster.

2.6 IoT-Based and Distributed Surveillance Systems:

Another approach is the integration of Internet of Things technology with the surveillance system. IoT-based systems use distributed sensors, cameras, and drones to provide surveillance over large areas such as borders and critical infrastructure. Surveillance systems using drones and computer vision can be used for large areas. Cloud-based systems can be used for centralized processing. However, the use of IoT-based systems faces challenges such as cost, power consumption, network dependency, and system maintenance. Reliability may be compromised in low-connectivity areas.

2.7 Challenges in Existing Systems:
Though there have been many advancements in the field of surveillance, the existing surveillance systems have many challenges to overcome. They are listed below: High dependency on deep learning models and the requirement for expensive hardware Difficulty in deploying the system in real time on low-cost devices Scalability challenges in large or remote areas High system complexity and maintenance requirements Privacy and ethical concerns These challenges in the existing surveillance systems clearly indicate the requirement for a more efficient and cost-effective surveillance system.

2.8 Motivation for VigilAI:
The motivation for the development of VigilAI stems from the limitations of the available systems. Unlike other systems, which rely on deep learning techniques, VigilAI uses a combination of traditional techniques and AI techniques. The proposed system uses background subtraction for motion detection, face recognition through efficient encoding techniques, and YOLO for object detection, specifically for vehicles. A multi-level threat detection technique is proposed for classifying the detected objects into low, medium, and high threat levels. Furthermore, the proposed system incorporates several features like buzzer, snapshot, and email for sending alerts in real-time. Also, the proposed system is highly efficient on hardware without the need for cloud dependency.

2.9 Summary:
The proposed work is based on the literature review, which shows that although deep learning techniques offer high accuracy, they lack practicality due to their high computational requirements. Traditional techniques offer efficiency and real-time performance but lack accuracy. VigilAI is proposed as a solution that incorporates the advantages of both techniques. It is highly practical, efficient, and cost-effective, making it highly suitable for implementation.

III. METHODS AND WORKING

The system works through a structured pipeline, where the real-time video inputs are analyzed and the potential threats are identified. The method minimizes the computing power used for analysis while maximizing the accuracy of detecting any danger.

Step 1: Video Capture
The video feed is captured from the device's web camera or mobile camera. Frames from the live video stream are processed one after the other.

Step 2: Motion Detection
Motion is identified using a background subtraction algorithm (MOG2). This is a filtering mechanism where further processing happens only when there is a substantial motion.

Step 3: Face Detection and Recognition
Once the motion is detected, faces in the frame are detected, facial encodings are created and matched against the stored encodings of known people.
Recognized face → Known individual
Unrecognized face → Unknown individual (Medium-level alert)

Step 4: Object Detection
The YOLO model detects objects like cars and animals. These objects are marked, and bounding boxes are drawn around them.
Cars → Potential intrusion signs
Animals → non-dangerous events

Step 5: Weapon Detection
The system uses a customized YOLO network for detecting firearms or handguns. In case of weapon detection, it would be categorized as a high-risk threat.

Step 6: Threat Assessment
Depending on the outcome of the detection phase, the threats would be categorized into:
Low Risk: Presence of animals or other non-threatening objects
Medium Risk: Presence of unidentified humans
High Risk: Detection of firearms

Step 7: Alerts
Based on the degree of risk, the system takes the following actions:
Alarm: Audible alarm signal generation.
Photo Capture: Captured image retained for documentation purposes.
Email: Sent along with the date and location stamp.
The Cooldown process is enabled to avoid multiple alerts within a short period of time.

Step 8: Log
All events are logged into a CSV file containing information such as time, detected object/person, risk category, and photo location.

3.1 System Overview:
VigilAI system has the following modules: Video Acquisition Module Motion Detection Module Face Recognition Module Object Detection Module Threat Classification Module Alert and Notification System.

3.2 System Architecture Workflow:
Camera → Motion Detection → Face Recognition → Object Detection → Threat Analysis → Alert System.

3.3 Motion Detection:
VigilAI system uses background subtraction techniques like MOG2 for motion detection. This helps in reducing processing power because the system processes the video only when motion is detected.

3.4 Face Recognition:
Face recognition in the system uses the face_recognition library. The known faces are stored in the dataset. The faces detected in the video stream are compared with the dataset.

3.5 Object Detection:
Object detection in the system uses the YOLO model. The system detects objects like vehicles and animals.
3.6 Gun Detection (Threat Module):
VigilAI system uses the YOLO model for the detection of guns. The system detects objects like guns, pistols, and rifles.

3.7 Multi-Level Threat Classification:
Threat levels in the system: Low Alert: Animals and objects detected Medium Alert: Unknown Person Detected High Alert: Weapon Detection.

3.8 Alert Mechanism Alert mechanism in the system:
Sound buzzer for immediate action Capture the snapshot of the detected face for evidence purpose Send email with the detected face and the date and time of detection.

IV. IMPLEMENTATION

The implementation of the VigilAI system is done by utilizing the Python programming language and libraries including OpenCV, face_recognition, and Ultralytics YOLO. The system starts by initializing the camera and loading pre-trained models. Known faces are stored and encoded during initialization. During runtime: Frames are continuously captured Motion detection filters out unwanted frames Face recognition is done to identify people Object detection is done to identify vehicles and animals Weapon detection is done to identify potential threats The events are stored in a CSV file, and images are stored in directories for future use.
The alert system is implemented by utilizing the SMTP library to send emails. This is done to avoid system blocking by implementing threading.

V. RESULTS AND DISCUSSION

The proposed system was implemented in various environments to test the efficiency of the system. The system was able to detect motion, recognize known individuals, and recognize unknown individuals. Object detection was successful in identifying vehicles and animals in various lighting conditions. The system was able to prove the efficiency of the weapon detection module in identifying high-risk objects. The accuracy of the system depends on the quality of the model. The alert system was efficient in generating buzzer alerts and email notifications with minimal delay. The cooldown feature was successful in preventing repeated alerts. The system was able to maintain the balance between efficiency and computational efficiency.

VI. CONCLUSION

This paper presented VigilAI, an intelligent border surveillance system designed to address the limitations of traditional monitoring systems. By integrating motion detection, face recognition, and object detection, the system provides an efficient and real-time solution for detecting suspicious activities. The introduction of multi-level threat classification enhances system responsiveness and prioritizes critical alerts. The use of lightweight techniques ensures that the system can operate effectively on

standard hardware, making it suitable for deployment in remote and resource-constrained environments. VigilAI demonstrates strong potential as a practical and scalable solution for modern surveillance applications.

REFERENCES

[1] Mr. N. Mohammed Haris, K. Naveen, GV. Vasundralakshmi, G. Pavatharani, AI Powered Smart Security Bordering System, Vol. 5, Issue 2, May 2025.
[2] Tosin Ige, Abosede Kolade, Olukunle Kolade, Enhancing Border Security and Countering Terrorism Through Computer Vision: A Field of Artificial Intelligence, Vol. 5, Issue 2, May 2025.
[3] Siham Boukhalfa, Abdelmalek Amine, Dr. Moulay Tahar, Border Security and Surveillance Using IoT, Vol. 12, AI for Border Control and Surveillance, Issue November 2023
[4] Jandarma ve Sahil Güvenlik Akademisi, Güvenlik Bilimleri Enstitüsü, An AI-Based Surveillance System Proposal for The Second Line Assessment, Vol. 12, Issue May 2024.
[5] OpenCV Library, https://opencv.org/ Adam Geitgey, face_recognition Python Library, GitHub Repository.
[6] H. Poor, An Introduction to Signal Detection and Estimation; New York: Springer-Verlag, 1985, ch.4.